Lecture 14: Problems and Solutions with Wi-Fi

Problems with Wi-Fi:

- Poor user interface for roaming; at each new Hot Spot, users have some annoying reconfiguring to do.
- Many fragmented and incompatible networks. If the Starbucks' network isn't the same specs as the airport's, you might be out of luck.
- User roaming authorization process (lengthy, complex). You may need to tattoo SSIDs, passwords and a litany of other information on your arm for repeated reference.
- Billing by the minute, single source billing. Imagine a separate bill for every different Hot Spot you used.
- Security. How to keep evesdroppers from eyeing your private network.

Some solutions.

Roaming: Users want to roam between WiFi and cellular networks, using the slower but more ubiquitous cellular data networks for places like trains, where WiFi access points may be unavailable. PCtel, which began life as a manufacturer of host-based analog PC modems, has moved into wireless with its Segue platform which allows roaming between different 802.11 environments, as well as between WLANs and cellular networks such as CDMA 1xRTT and GPRS. A separate controller solution handles AAA processing. Intel, in addition, sees roaming as a critical element in its wireless future. Intel already supplies the majority of flash chips in cell phones, many of the industry's microcontrollers, and will shortly add baseband chips to the mix.

Billing: Pass-One and Gric allow users to roam WiFi networks worldwide with a one-stop pricing model charging on a per-Kbyte or per-minute basis, or an unlimited use plan. The whole theory is that if a user belongs to one portal who wants to roam onto another, he still belongs to one provider like Pass-One or Gric. The system provides him a welcome screen with a roaming button and keeps tab on what cost he'll incur by connecting to a location. The system onto which the user is roaming, however, must be able to authenticate the user, measure his usage, and pass along the bill to the original portal. The system must also take into account companies in various parts of the world.

Security: Basic things to do-

- Turn on WEP (Wired Equivalent Privacy)
- Change Your Default Password
- Close Your Network (If Possible)
- Change Your Network Name
- Move Your Access Point
- Use MAC Control Tables
- Other Simple Solutions
- Use a VPN (Virtual Private Network)

Most important: Turn on WEP (Wired Equivalent Privacy)

WEP is the underlying security technology provided by the Wi-Fi (802.11b) standard. Even though WEP is not perfect, it does provide basic security. Some experts say that from 60 to 80 percent of all wireless LAN networks operate with WEP not turned on.

Most home and small office Wi-Fi systems provide 40-bit (also called 64-bit) WEP encryption. To make initial installation simple, most Wi-Fi access points ship with WEP turned off. So once you have your network turned on and working, make sure you activate WEP by following the instructions in your manufacturer's instructions.

You can also increase your security by periodically changing the encryption key. If you're concerned about privacy, change your code every week or two. If you're very concerned, change it more often or use an advanced security technology such as 802.1x, which can change your WEP code automatically every 5 minutes or so.

Change Your Default Password

Most wireless networks ship with a default password provided by the manufacturer. Change it as soon as possible. Most hackers can easily figure out the default password once they identify the make of your network access point.

Close Your Network (If Possible)

If possible, block the SSID (Service Set Identifier) from being broadcast. This has the effect of "closing" your network. Many Wi-Fi systems enable you to close the network.

All access points ship with a wireless beacon signal so that wireless PCs can more easily find them. In effect, the signal is shouting, "I'm here! Log on!" By turning the SSID off or by "closing" your network, you make it much harder for hackers to find you: If they don't know your network exists, there's less chance they will spend the time to crack your communications. So, If your equipment permits you to close the network, make sure you do so.

Change Your Network Name

Most access points ship with a default network name. When your network is up and running you should change the name to something personal, yet hard to guess. In other words, if your last name is Smith, don't call it the Smith network. Many companies, even large corporations, label their network with their company name or their address. Don't

do it. Be creative. A combination of letters and numbers is recommended, but don't use your street address!

Move Your Access Point

To increase privacy, place your access point in the middle of the room, away from open windows and doors. The more metal and wood you put in the way, the less distance your wireless messages can travel. You can test how much of your signal is escaping from your business or home by taking your Wi-Fi equipped laptop outside (for a site survey) and checking to see how far you can go and still make a connection. You might be surprised.

Use MAC Control Tables

Use MAC (Medium Access Control) tables if your access point supports them. Like all networking devices, a Wi-Fi radio, has a unique MAC address coded into its memory. By using the MAC Access Control List (ACL), you can limit the wireless connection to only those Wi-Fi radios whose MAC addresses are directly enabled in your access point. It's like call blocking on a telephone, but for a wireless LAN. If a rogue wireless radio with a MAC address that is not in this table tries to connect to your network, your access point will not let it.

Other Simple Solutions

There are various ways to set up your computer's directories and network to protect your stored files and data. One way is to turn off "Sharing" and use "Passwords" to access directories holding confidential files. Sharing and Passwords are accessed in Windows by right clicking on the directory and going to the "Properties" command. Remember that most web sites that handle purchases, credit cards and other financial information usually use encryption methods such as SSL(secure socket layer) to protect sensitive data, financial data for instance.

Use a VPN (Virtual Private Network)

A VPN creates a virtual tunnel from your computer through the local wireless access point, through the Internet, and then to your corporate headquarters. Even though it can be complicated and expensive, using VPN creates an almost impenetrable wall of security for your wireless communications whether you're working from home, an airport

lounge or your company's meeting rooms. VPNs are commonly used today to provide remote workers with access to the enterprise network via the Internet. In addition, VPNs can be used to provide wireless clients with access to the wireless network. There are two main advantages of this approach. The VPN provides a secure and manageable access method, and users have a single VPN interface for remote and wireless access to the enterprise network

Notes:

War driving—a term hackers use for discovering wireless networks while moving around in an area. With a wireless radio with netsniffing software, one can find out the manufacturer, service set identification (SSID), media address control (MAC), signal strength, channels and whether authentication and encryption (WEP) were set on or off for the various wireless access points out there. These vital statistics are what "war drivers" look for, as they allow potential launch of denial-of-service (DoS) attacks that overload the access point, thus making it unable to service requests of wireless clients who are requesting for authentication.

Currently, WEP and MAC filtering (the latter is a lot of tedious work) alone may not be enough for securing your wireless network. However, when combined with more robust methods of authentication, such as 802.1x using extensible authentication protocol (EAP) and remote authentication dial-in user service, you can get a more reliable and secured communication channel. Also using WEP with encryption and decryption algorithms can cause performance degradation.